Current Claim Schedule

Claims 1-24 (cancelled).

25. (Currently Amended) A method of electronically issuing an electronic negotiable document (END) comprising: creating as data an END and storing this in ~~a~~ tamper-resistant document carrier hardware, the document carrier hardware containing a unique public-secret key pair for signing and verifying, ~~the secret key being generated within the document carrier,~~ and a unique document carrier identifier; signing the unique document-carrier identifier, the END and an END identifier using the secret key of the public-secret key pair, and storing the result in the document carrier hardware.

26. (Currently Amended) A method according to Claim 25 of issuing an END, further comprising generating a time stamp representing the time of issue and storing this with the END in the tamper-resistant document carrier hardware before the ~~encryption~~ signing step.

27. (Currently Amended) A method according to Claim 25 of issuing an END, including the step of calculating a hash value of the END and/or the time stamp value and storing this hash value instead of the full END in the tamper-resistant document carrier hardware, before the said ~~encryption~~ signing step.

28. (Previously Presented) A method according to Claim 25 of issuing an END, in which the document carrier identifier is a device number and the END identifier is a serial number.

29. (Currently Amended) A method according to ~~claim~~ Claim 25 of issuing an END, in which the END identifier is supplemented with data representing a water mark unique to the issuer.

30. (Currently Amended) A method according to ~~claim~~ Claim 25 of issuing an END, comprising the step of calculating a hash value of the data to be ~~encrypted by~~ signed using said secret key, in place of the full data.

31. (Currently Amended) A method according to ~~claim~~ Claim 25 of issuing an END, in which the document carrier hardware stores a negotiability status flag indicative of whether the END stored therein ~~in~~ is negotiable or non-negotiable, and including the step of setting the flag to "negotiable" after the result of the encryption has been stored in the document carrier hardware.

32. (Currently Amended) A method according to ~~claim~~ Claim 25 of issuing an END, in which the document carrier hardware includes a counter for counting a serial number, indicative of the number of times that the END has been negotiated since issue, and comprising the step of setting the counter to zero after the result of the encryption has been stored in the document carrier hardware.

33. (Currently Amended) ~~A tamper~~ Tamper-resistant document carrier hardware adapted to store an END in accordance with the method of ~~claim~~ Claim 25, said hardware comprising read only software for controlling the steps of storing the END, encrypting the END and other data with the pre-stored secret key, and storing the result in a memory.

34. (Currently Amended) ~~A document~~ Document carrier hardware according to Claim 33, in which the memory includes a negotiability status flag capable of being set either to "negotiable" or to "non-negotiable'.

35. (Currently Amended) ~~A document~~ Document carrier hardware according to Claim 33, in which the memory includes a counter for storing a serial number representative of the number of times the END has been negotiated.

36. (Currently Amended) A method of electronically negotiating an END between a seller and a buyer each possessing ~~a~~ tamper-resistant document carrier hardware having its own public-secret key pair, in which the END is stored in the seller's document carrier hardware in the form of END data, and the signature generated by the secret signing-key of a document carrier of the issuer of the END, together with a negotiability status flag indicative of whether the END is currently negotiable from the document carrier hardware on which it is stored, comprising establishing mutual recognition between the seller and buyer using one or more predetermined protocols between the ~~respective~~ buyer's and seller's document ~~carriers~~ carrier hardwares; verifying in the seller's document carrier hardware that the negotiability status flag is "negotiable" and aborting the negotiation if not; sending the public encryption key of the buyer's document carrier hardware to the seller's document carrier hardware, and using it to encrypt the message comprising the END together with the negotiability status flag; sending that encrypted message to the ~~buyer~~ buyer's document carrier hardware; decrypting that message using the buyer's secret decryption key, and setting the negotiability status flag for that END of the buyer's and seller's document ~~carriers~~ carrier harwares respectively to ~~"non-negotiable"~~ "negotiable" and ~~"negotiable"~~ "non-negotiable".

37. (Currently Amended) A method of electronically negotiating an END between a seller and~~,~~ a buyer each possessing a tamper-resistant document carrier hardware having its own public-secret key pair, in which the END is stored in the seller's document carrier hardware in the form of END data, and the signature generated by the secret signing key of a document carrier hardware of the issuer of the END, together with a serial number counter indicative of the number of times that the END has been negotiated since issue, comprising establishing mutual recognition between seller and buyer using one or more predetermined protocols between the ~~respective document carriers~~ buyer's and seller's

document carrier hardwares verifying in the seller's document carrier hardware that the END, if it has been stored previously in that document carrier hardware, has a different counter value this time and is therefore negotiable; sending the public encryption key of the buyer's document carrier hardware to the seller's document carrier hardware, and using it to encrypt the message comprising the END together with the counter; sending that encrypted message to the ~~buyer~~ buyer's document carrier hardware;decrypting that message using the buyer's secret decryption key, and incrementing the counter by one.

38. (Currently Amended) A method according to Claim 36, in which each document carrier hardware is installed originally with a certificate comprising a digital signature of its unique identifier and of its public key.

39. (Currently Amended) A method according to Claim 37, in which each document carrier hardware is ~~in-stalled~~ installed originally with a certificate comprising a digital signature of its unique identifier and of its public key.

40. (Currently Amended) A method according to Claim 38, in which the certificate unique to the document carrier hardware on which the END was originally issued is stored with the END in the seller's document carrier hardware.

41. (Currently Amended) A method according to Claim 39, in which the certificate unique to the document carrier hardware on which the END was originally issued is stored with the END in the seller's document carrier hardware.

42. (Currently Amended) A method according to Claim 38, in which the certificate of the buyer's document carrier hardware is sent to the seller's document carrier hardware in which it is authenticated and the negotiation is aborted if authentication fails.

43. (Currently Amended) A method according to Claim 39, in which the certificate of the buyer's document carrier hardware is sent to the seller's document carrier hardware in which it is authenticated and the negotiation is aborted if authentication fails.

44. (Currently Amended) A method according to Claim 36, in which the buyer's document carrier hardware, after decrypting the message using its secret key, verifies the signature of the issuer on the END, and informs the issuer in the event that authentication fails.

45. (Currently Amended) A method according to Claim 37, in which the buyer's document carrier hardware, after decrypting the message using its secret key, verifies the signature of the issuer ~~on~~ of the END, and informs the issuer in the event that authentication fails.

46. (Currently Amended) A method according to Claim 25, of issuing an END on ~~a~~ document-carrier hardware followed by a method of negotiating an END between a seller and a buyer each possessing ~~a~~ tamper-resistant document carrier hardware having its own public-secret key pair, in which the END is stored in the seller's document carrier hardware in the form of END data, and the signature generated by the secret signing-key of a document carrier hardware of the issuer of the END, together with a negotiability status flag indicative of whether the END is currently negotiable from the document carrier hardware on which it is stored, comprising establishing mutual recognition between the seller and buyer using a predetermined protocol between the ~~respective~~ buyer's and seller's document ~~carriers~~ carrier hardwares; verifying in the seller's document carrier hardware that the negotiability status flag is "negotiable" and aborting the negotiation if not; sending the public encryption key of the buyer's document carrier hardware to the seller's document carrier hardware, and using it to encrypt the message comprising the END together with the negotiability status flag; sending that encrypted message to the ~~buyer~~ buyer's document carrier hardware; decrypting that message using the buyer's secret decryption key, and setting the negotiability status flag for that END of the buyer's

and seller's document ~~carriers~~ carrier hardwares respectively to "non-negotiable" and "negotiable".

47. (Currently Amended) A method according to Claim 25, of issuing an END on a document-carrier hardware followed by a method of negotiating an END between a seller and a buyer each possessing ~~a~~ tamper-resistant document carrier hardware having its own public secret key pair, in which the END is stored in the seller's document carrier hardware in the form of END data, and the signature generated by the secret signing key of a document carrier hardware of the issuer of the END, together with a serial number counter indicative of the number of times that the END has been negotiated since issue, comprising establishing mutual recognition between seller and buyer using a predetermined protocol between ~~their respective document carriers~~ the buyer's and seller's document carrier hardwares; verifying in the seller's document carrier hardware that the END, if it has been stored, previously in that document carrier hardware, has a different counter value this time and is therefore negotiable, but aborting the negotiation if it is not negotiable; sending the public encryption key of the buyer's document carrier hardware to the seller's document carrier hardware, and using it to encrypt the message comprising the END together with the counter; sending that encrypted message to the ~~buyer~~ buyer's document carrier hardware; decrypting that message using the buyer's secret decryption key, and incrementing the counter by one.

48. (Currently Amended) A method according to Claim 26, of issuing ~~and~~ an END on a document- carrier hardware followed by a method of negotiating an END between a seller and a buyer each possessing ~~a~~ tamper-resistant document carrier hardware having its own public-secret key pair, in which the END is stored in the seller' s document carrier hardware in the form of END data, and the signature generated by the secret signing-key of a document carrier hardware of the issuer of the END, together with a negotiability status flag indicative of whether the END is currently negotiable from the document carrier hardware on which it is stored, comprising establishing mutual recognition between the seller and buyer using a predetermined protocol between the ~~respective document car-~~

~~riers~~ buyer's and seller's document carrier hardwares; verifying in the seller's document carrier hardware that the negotiability status flag is "negotiable" and aborting the negotiation if not; sending the public encryption key of the buyer's document carrier hardware to the seller's document carrier hardware, and using it to encrypt the message comprising the END together with the negotiability status flag; sending that encrypted message to the ~~buyer~~ buyer's document carrier hardware, decrypting that message using the buyer's secret decryption key, and setting the negotiability status flag for that END of the buyer's and seller's document ~~carriers~~ carrier hardwares respectively to "non-negotiable" and "negotiable".

49. (Currently Amended) A method according to Claim 26, of issuing an END on a document-carrier hardware followed by a method of negotiating an END between a seller and a buyer each possessing ~~a~~ tamper-resistant document carrier hardware having its own public secret key pair, in which the END is stored in the seller's document carrier hardware in the form of END data, and the signature generated by the secret signing key of a document carrier hardware of the issuer of the END, together with a serial number counter indicative of the number of times that the END has been negotiated since issue, comprising establishing mutual recognition between seller and buyer using a predetermined protocol between ~~their respective document carriers~~ the buyer's and seller's document carrier hardwares; verifying in the seller's document carrier hardware that the END, if it has been stored previously in that document carrier hardware, has a different counter value this time and is therefore negotiable, but aborting the negotiation if it is not negotiable; sending the public encryption key of the buyer's document carrier hardware to the seller's document carrier hardware, and using it to encrypt the message comprising the END together with the counter; sending that encrypted message to the ~~buyer~~ buyer's document carrier hardware; decrypting that message using the buyer's secret decryption key, and incrementing the counter by one.

50. (Currently Amended) A method according to Claim 48, in which the buyer's document carrier hardware, after decrypting the message with its secret key, verifies that the

END is still valid by taking its time stamp, and, if it has expired, informs the issuer of this, and aborts the negotiation before ~~implementing~~ incrementing the counter or setting the negotiation status flag.

51. (Currently Amended) A method according to Claim 49, in which the buyer's document carrier hardware, after decrypting the message with its secret key, verifies that the END is still valid by taking its time stamp, and, if it has expired, informs the issuer of this, and aborts the negotiation before ~~implementing~~ incrementing the counter or setting the negotiation status flag.

52. (Currently Amended) A method according to Claim 36, including recovering the negotiation of an END which has previously broken down, by providing the buyer's document-carrier hardware with the necessary secret key which has been reproduced by the issuer or by a trusted third party.

53. (Currently Amended) A method according to Claim 37, including recovering the negotiation of an END which has previously broken down, by providing the buyer's document-carrier hardware with the necessary secret key which has been reproduced by the issuer or by a trusted third party.

54. (Currently Amended) A method according to Claim 36, including recovering an END lost from [[a]] primary document-carrier hardware, by activating ~~a~~ back-up document-carrier hardware [["]]which has previously been provided with back-up data reproduced from the primary document-carrier hardware.

55. (Currently Amended) A method according to Claim 37, including recovering an END lost from [[a]]primary document-carrier hardware, by activating ~~a~~ back-up document-carrier hardware which has previously been provided with back-up data reproduced from the primary document-carrier hardware.

56. (Previously Presented) A method according to Claim 52, comprising inhibiting the recovery until the expiry of the predetermined period of validity of the END.

57. (Previously Presented) A method according to Claim 53, comprising inhibiting the recovery until the expiry of the predetermined period of validity of the END.

58. (Previously Presented) A method according to Claim 54, comprising inhibiting the recovery until the expiry of the predetermined period of validity of the END.

59. (Previously Presented) A method according to Claim 55, comprising inhibiting the recovery until the expiry of the predetermined period of validity of the END.

60. (Currently Amended) A method of electronically negotiating an END, sold by a seller to a buyer, in which the buyer splits the END electronically into two or more parts and then negotiates those parts separately to one or more further buyers.

61. (Currently Amended) A method according to Claim 60, in which each part is subjected to the digital signature of the ~~said buyer's~~ document carrier hardware of said buyer which effects the splitting.